Mandiant

ON-DEMAND INTELLIGENCE TRAINING

On-Demand Intelligence Training is a cost-effective way to empower cyber security teams to effectively use intelligence across different job roles, at different skill levels. Courses include videos led by FireEye subject matter experts and practitioners, written texts, and interactive assessments.

Service Overview

On-Demand Intelligence training is available for anyone to purchase, including individuals and non-clients. Students can view and purchase courses from the Mandiant training website or through their sales representative at $1,000/seat/course or 1 EOD credit, and courses can be accessed for 3 months from the date of registration. Currently available courses include: **Cyber Intelligence Foundations (CIF)**, **Intelligence Research I (Scoping),** and **intelligence Research II: Open Source Intelligence (OSINT) Techniques and Tools.**

Service Activity and Details

Students can purchase courses from the **Mandiant Course Registration website (https://www.mandiant.com/academy/course-registration)** using a credit card. Organizations looking to purchase bulk licenses can work with their sales representative to purchase at a discount. Seats are non-transferrable. Once students purchase their courses, they will receive an automated email with instructions to complete their registration by setting up the required multi-factor authentication. To report errors, students should contact **AdvantageTraining@mandiant.com ()**

Each course has between 8 and 32 hours of content, and align to a different phase of the Intelligence Lifecycle.

Available Courses

Course	Description	Content (Hours)
Cyber Intelligence Foundations (CIF)	A foundational survey course that introduces the field of cyber intelligence. All subsequent courses reinforce concepts introduced here.	32
Intelligence Research I (Scoping)	Aligns to Planning and Direction Phase of Intelligence Lifecycle. Learn how to ask the right questions and identify relevant context to properly scope an RFI, assess sources, and utilize a Research Management System.	8
Intelligence Research II (OSINT Tools and Methods)	Aligns to Collection & Processing Phase of Intelligence lifecycle. Learn how to leverage open-source tools to identify and think critically about pivot points to drive investigations across multiple use cases.	16
Intelligence Production	Aligns to Production Phase of Intelligence lifecycle. Learn how to structure, compose, and edit intelligence products and briefings by deconstructing a series of vendor reports.	8

Cyber Intelligence Foundations (CIF)

This foundational course provides a wide-ranging introduction to Cyber Intelligence roles, frameworks, tradecraft, and organizational value. Students will uncover the different ways intelligence can drive value across many different use cases. They will receive a high-level programmatic overview of intelligence, including team composition, the organizational role of cyber threat intelligence (CTI), and stakeholder analysis.

Content also includes basic practitioner skills such as developing raw data into minimally viable intelligence, interpreting cyber artifacts, and leveraging the intelligence cycle to compose original intelligence products. Students will also receive an introduction to basic attribution techniques.

Cyber Intelligence Foundations is the cornerstone of the Intelligence Training offerings. Concepts introduced in this course are reinforced and explored more in-depth in subsequent intelligence training courses.

Prerequisites: None

Who Should Attend: This is a foundational level course for anyone looking to get started with cyber intelligence, as a practitioner or consumer.

Module	Key Topics*
Introduction to Cyber Threat Intelligence	Definition of Cyber Threat Intelligence; different collaborative roles (SOC, NOC, VAT, IR, etc.); levels of intelligence; Threat Modeling, Threat Modeling
The Analyst's Toolkit	Dual Process Theory; Intuitive versus Analytic; Wason Selection Task; Ambiguity Effect; Types of Bias (confirmation, conservatism, etc.); Groupthink; Failure to Consider Visibility; Source Reliability/Fidelity; Failure to Account for Human Action; Estimative Language
Cyber Artifacts	Cyber Key Terrain; File-based; Network-based; Host-based; Binary; Backdoor;Botnet; Downloader; Dropper; Ransomware; Infostealer; Rootkit; Worm; Compile; File Hash; Strings; Packer; Obfuscation; Compression; IOC's in Modeling
Developing Raw Data into Minimally Viable Intelligence	Develop Source Data; Threat Documentation; Blue, Red, Green, and Yellow; ANB Charts; Common Operating Picture (COP); Analyst's Notebook; Maltego; Sharepoint; MediaWiki; Anchor Node; FQDN; Pyramid of Pain
How Intelligence Teams work with Malware	Production Systems; AirDrop; USB; SecureFile; Static Analysis; Dynamic Analysis; Hashing; Strings; Sandboxing
Writing Intelligence Products	Technical Writing; Knowing your Audience; Critical Thinking for Establishing Audience; Review Procedures; BLUF; AIMS
Establishing Attribution	Basic Modeling Techniques; Levels of Attribution; Natural Language; Nodes and Edges; Graph Database

Intelligence Research I (Scoping)

This foundational course teaches students to analyze, prioritize, and fully understand Requests for Information (RFI's), and create a research plan that keeps their efforts on track.

Students will learn how to ask the right questions to uncover stakeholder intent, ensuring their intelligence analysis can be actioned. They will learn to identify relevant context to fully interpret implicit and explicit RFI's by reviewing intelligence requirements, organizational threat profiles, and key stakeholder analysis.

They will also learn how to leverage a Research Management system to organize their research and avoid information overload, and methods for assessing source relevance and trust to ensure up front their collections efforts are efficient and focused on the task at hand.

Prerequisites: Students should have taken Cyber Intelligence Foundations, or have equivalent knowledge.

Who Should Attend: This is a foundational level course for cyber practitioners who must scope and respond to formal and informal Requests for Information (RFI's).

Module	Key Topics
Organizing Research	Research Goals and Objectives; Key Considerations of Research; Explicit and Implicit prompts; Essential Elements of Information; 4 Step Research Process (Prompt, Plan, Gather Evaluation), Intelligence Requirements, Threat Profile, Key Stakeholder Analysis, Context, Priority
Assessing Information	Interrogating Existing Holdings; Intelligence Gaps, Knowledge Management Practices, Working Knowledge of Environment; Source Types; Key Characteristics of Sources; Stakeholder and Influence Mapping; Relevance; Trust; Admiralty Code (Reliability + Credibility); Source Bias; Facts v. Opinion v. Assessment; Estimative Language; Cognitive Bias
Capstone	Outline a research response for a scenario tied to Triton activity

Intelligence Research II: Open Source Intelligence (OSINT) Techniques and Tools

This foundational course teaches students to identify and develop pivot points or leads in investigations across multiple use cases. Students will learn when and why to leverage an open source tool in their research, and review basic functionalities. They will think critically about how to push their research further across several scenarios drawn from front line experience, including response to executive-level RFI's, incident response investigations, and information operation campaigns.

As they work through these scenarios in a lab environment, students will apply their knowledge of tools such as VirtusTotal, Alienvault, PassiveTotal, and Facebook, and utilize advanced search engine techniques.

Prerequisites: Students should have taken Cyber Intelligence Foundations and Cyber Research I (Scoping) or have equivalent knowledge.

Who Should Attend: This is a foundational level course for cyber practitioners who must safely and efficiently conduct research as part of investigations or in response to RFI's.

Module	Key Topics
OSINT Overview	Definitions, values/dangers, critical thinking framework (Scope, Identify/Harvest, Normalize, Enrich, Synthesize, Report), OODA LOOP
Getting your Systems Started	OPSEC, configuring your PC, toolbars and add-ons, mindmaps, case notes, VM's
Tools and Techniques	Virustotal, Search Engines (Google Dorking, Hacking Database,Reverse Image Search, Censys, Fofa, Dogpile, Archives); Shodan; PassiveTotal; DomainTools; Social Media (API's, Facebook, Twitter, Sock Puppets); Government documents; Deleted Data (Way Back Machine, Cached Pages, Screenshots.com); Image/Video Metadata; Usernames/Aliases (checkuser.org, namechk.com)
Capstone	Apply learned skills to a scenario utilizing a virtual machine

Mandiant Responsibilities

In addition to the activities described thus far, Mandiant is responsible for the following:

- Managing all aspects of the customer experience, including payment processing, managing the Learning Management System (LMS) and all student account details
- For organizations purchasing in bulk, Mandiant will provide upon request metrics tied to student completion and performance
- Providing a certificate to all students who complete the courses and score above 75% on the course exam (students can re-take this exam as many times as necessary)

Customer Obligations

Customer obligations for this service are as follows:

- Licenses are non-transferrable. Students should not share information or materials from the platform.
- Licenses can not be canceled once students access the course for the first time. Students should carefully review all course outlines, sample videos, and sample lessons prior to purchase, to ensure the course meets expectations.

Out-of-Scope

The following are considered out-of-scope for this service.

- Questions to instructors on content
- Requests for additional information
- Requests for analytic support
- Access to intelligence reporting beyond the content included as case studies and exercises within the courses

Additional Education Services

Mandiant offers numerous training services beyond intelligence training, including teacher-led and web-based training. The full catalog is available on the Mandiant Academy training website: **https://www.mandiant.com/academy**.